

**REMARKS**

The Office Action dated January 12, 2004 has been reviewed and carefully considered. Claims 1-17 remain pending in the application, of which the independent claims are 1, 2, 8 and 13. Reconsideration of the above-identified application in view of the following remarks is respectfully requested.

Claims 1, 2 and 4-7 stand rejected under 35 U.S.C. 103(a) as unpatentable over International Publication Number WO 98/56179 to Eskicioglu et al. ("Eskicioglu") in view of ITU-T Recommendation H.222.0 (hereinafter "ITU-T") and U.S. Patent No. 5,987,126 to Okuyama et al. ("Okuyama").

Claim 1 recites, "each control information pair having copy control information and a stream identifier, respectively generating a first key in the point of deployment module and a second key in the set-top box, using the at least one control information pair."

Eskicioglu fails to disclose or suggest the above-quoted "generating . . . a first key . . . in the . . . module . . . and a second key . . . in the . . . box." The reference merely says that a smart card 30 uses (page 8, line 28: "used") one key to encrypt and that a set top box 20 uses (page 9, line 19: "using") another key to decrypt. Nor is there the slightest inkling as to why the non-disclosed generating would be "using the at least one control information pair" as explicitly required by the language of claim 1. None of the other applied references make up for these deficiencies. Instead, bits and pieces of disclosure have been strung together in an incredible combination whose motivation can only be understood as impermissible hindsight by the Examiner based on the instant application. Accordingly, for at least these reasons, the invention as recited in claim 1 is

not rendered obvious by the proposed combination of prior art references.

Reconsideration and withdrawal of the rejection is respectfully requested.

Claim 2 likewise recites, “each pair having a copy control information and a stream identifier; (c) generating a first shared key at the host and a second shared key at the deployment module, respectively, using the at least one control information pair and an encryption means.” Accordingly, claim 2 distinguishes patentably over the applied prior art for at least the same reasons set forth above with regard to claim 1.

Claim 3 stands rejected under 35 U.S.C. 103(a) as unpatentable over Eskicioglu in view of ITU-T, Okuyama and “Communications Engineering & Design” by Lafferty.

Claim 3 depends from claim 2. Lafferty cannot compensate for the shortcomings of the other references. Accordingly, the proposed combination of references fails to render obvious the invention as recited in claim 3.

Claims 8-17 stand rejected under 35 U.S.C. 103(a) as unpatentable over U.S. Patent No. 6,055,314 to Spies et al. (“Spies”) in view of ITU-T and Okuyama.

Claim 8 recites, “the reply message including at least one control information pair, each pair having copy control information and a stream identifier, generating a first shared key using the at least one control information pair.”

The applicants fail to find any support for the proposition that Spies discloses or suggests “generating . . . using . . . at least one control pair,” as suggested at page 9 of the Office Action which refers to “fig. 6, ref. num 118.”

Moreover, what in the three references suggests the idea of “the reply message including at least one control information pair, each pair having copy control

information and a stream identifier, generating a first shared key using the at least one control information pair?” The Office Action suggest at the top of page 11 that motivation exists for meeting this limitation “because copy control information signifies to the method which level of copy protection to maintain.” This purported motivation, however, fails to explain, for example, at least why said generating uses a pair, one element of the pair happens to be copy control information, and said reply message also contains the copy control information.

Once again, bits and pieces of various disclosures are construed to form a combination which is incredible if not for impermissible hindsight of the Examiner based on the current application. Accordingly, the proposed combination of references fails to render obvious the invention as recited in claim 8.

Claim 13 likewise recites the same above-quoted limitations, and is patentable.


As for the other rejected claims, each depends from a base claim and is patentable at least due to its dependency, although each warrants additional consideration on the basis of its individual, further merits.

For all the foregoing reasons, it is respectfully submitted that all the present claims are patentable in view of the cited references. A Notice of Allowance is respectfully requested.

Respectfully submitted,

Dan Piotrowski  
Registration No. 42,079

Date: 4/7/04

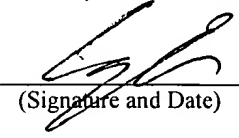
  
By: Steve Cha  
Attorney for Applicant  
Registration No. 44,069

**Mail all correspondence to:**  
Dan Piotrowski, Registration No. 42,079  
US PHILIPS CORPORATION  
P.O. Box 3001  
Briarcliff Manor, NY 10510-8001  
Phone: (914) 333-9624  
Fax: (914) 332-0615

**Certificate of Mailing Under 37 CFR 1.8**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to MAIL STOP NON-FEE AMENDMENTS, COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA. 22313 on 4/7/04.

Steve Cha, Reg. No. 44,069  
(Name of Registered Rep.)

  
(Signature and Date)